(19)日本国特許庁（ＪＰ）　(12)公開特許公報(A)　(11)特許出願公開番号

特開平4－245368

(43)公開日　平成4年(1992)9月1日

(51)Int.Cl.[5]		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ	15/00	３３０　Ｚ	7323－5L		
	12/00	５３７　Ｈ	8944－5B		
	15/40	５３０　Ｐ	7056－5L		
Ｇ０９Ｃ	1/00		7922－5L		

審査請求　未請求　請求項の数３(全　7　頁)

(21)出願番号　特願平3－10267

(22)出願日　平成３年(1991)１月31日

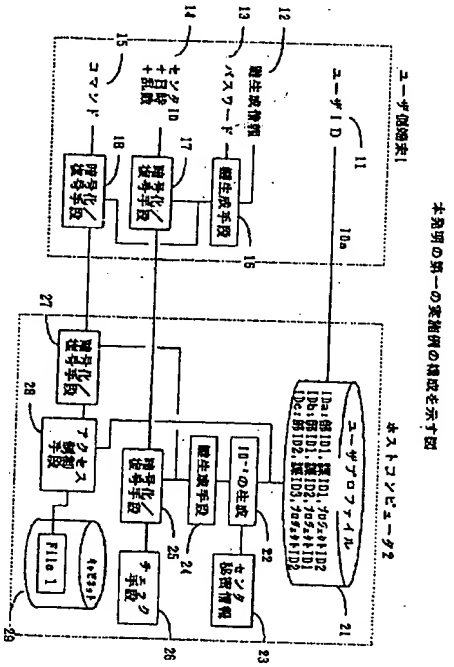
(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地
(72)発明者　長谷部　高行
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内
(74)代理人　弁理士　井桁　貞一

(54)【発明の名称】　電子ファイルキャビネットシステム

(57)【要約】

【目的】本発明は分散処理システムにおいてホストコンピュータが電子ファイルキャビネットを管理するシステムに関し、ログイン制御、アクセス制御、暗号化方法の各技術を一元的に管理することにより、安全性、利便性に優れたシステムの提供を目的とする。

【構成】ユーザ側端末には、ユーザ識別情報を送出する手段と、ユーザ識別情報や各ファイルの識別情報とパスワードとにより生成される公開鍵を入力する手段と、該公開鍵とパスワードとを基に第一の秘密鍵を生成する手段とを設けて該秘密鍵これにより暗号化を行い、またホストコンピュータには受信したユーザ識別情報によりファイル識別情報を出力するユーザプロファイルと、ユーザ識別情報およびファイル識別情報とにより第二の秘密鍵を生成する手段とを設けて該秘密鍵を設けて復号を行なうように構成して、ログイン制御、アクセス制御を一元化する。



本発明の第一の実施例の構成を示す図

1

【特許請求の範囲】

【請求項1】ユーザ側の端末（1）と、該端末（1）から送出された要求に基づいてホストコンピュータ（2）が電子ファイルキャビネット（29）をアクセスするシステムにおいて、前記端末（1）側には、ユーザを識別するためのユーザ識別情報を入力して前記ホストコンピュータ（2）側に送出する手段（11）と、ユーザの秘密情報と前記電子ファイルキャビネットを特定化するファイル識別情報とを構成要素として含み作成された公開鍵を入力する手段（12）と、前記公開鍵とユーザにより入力される前記秘密情報とに基づいて第一の秘密鍵を生成する手段（16）と、入力された該認証情報を前記秘密鍵を用いて暗号化して前記ホストコンピュータ（2）に送出する手段（17）と、入力されたファイルアクセスコマンドを前記第一の秘密鍵を用いて暗号化して前記ホストコンピュータ（2）に送出する手段（18）とを有し、前記ホストコンピュータ（2）は、前記ユーザ識別情報毎にアクセス権限が与えられたファイルのファイル識別情報が格納されるユーザプロファイル（21）と、前記ユーザプロファイル（21）から読みだされる識別情報を基に第二の秘密鍵を作成する手段（22，23，24）と、前記第二の秘密鍵を用いて前記暗号化された認証情報を復号する手段（25）と、前記復号した認証情報の正当性をチェックして端末（1）のログインを許可／不許可を行う手段（26）と、前記第二の秘密鍵を用いて前記暗号化されたコマンドを復号する手段（27）と、前記復号されたコマンドを基に前記ユーザプロファイル（21）を参照し、アクセス権限を確認して前記電子ファイルキャビネット（29）をアクセスするアクセス制御手段（28）を有することを特徴とする電子ファイルキャビネットシステム。

【請求項2】前記公開鍵は、所定の整数をベキ乗して得られるデータ値であり、該ベキ乗の項には前記秘密情報の逆数と前記識別情報の逆数とが積の項が含まれ、前記第一の鍵生成手段（16）は、入力された前記秘密情報を用いて前記公開鍵から前記秘密情報の逆数の項を消すことにより前記第一の秘密鍵を生成し、前記第二の鍵生成手段（22，23，24）は、センタ秘密情報（23）を用いて前記各識別情報の逆数を生成し、得られた各識別情報の逆数を項として用いて前記所定の整数のベキ乗演算を行うことにより第二の秘密鍵を生成することを特徴とする請求項1に記載の電子ファイルキャビネットシステム。

【請求項3】前記ホストコンピュータ（2）は、前記ユーザプロファイル（21）中の各識別情報の項には該識別情報が更新されたか否かを示す更新情報を設けると共に、更新された識別情報と更新される前の識別情報との対応関係を記憶する変更識別情報保持手段（31）を設け、受信したユーザ識別情報によりユーザプロファイル（21）から各識別情報を読みだす際には前記更新情報

2

をチェックして、更新がなされている場合は前記変更識別情報保持手段（31）を読みだして得られる新しい識別情報を含む公開鍵生成情報を作成し、この公開鍵生成情報を前記第二の秘密鍵を用いて暗号化してログインを許可した端末に送出し、その後で前記ユーザプロファイル（21）のうち更新すべき識別情報の項を新しい識別情報に書換えるよう構成し、前記端末（1）は、前記暗号化された公開鍵生成情報を前記第一の秘密鍵を用いて復号して、公開鍵を更新するように構成したことを特徴とする請求項1に記載の電子ファイルキャビネットシステム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明はＩＤベースファイル暗号用鍵管理方式を用いた電子ファイルキャビネットに関する。

【0002】

【従来の技術】分散処理システムにおいては、ワークステーション及びパーソナルコンピュータ等のデータを格納する、即ち電子ファイルキャビネットとしての役割がホストコンピュータに求められている。

【0003】一方、多数の人がアクセスを行うホストコンピュータにデータを蓄積することは，第３者によるデータのアクセスの危険性があることであり，これを保護するためには，暗号化・アクセス制御等の技術が必要である。

【0004】従来のアクセス制御による電子ファイルキャビネットの管理システムを図Ａに示す。図中、１００は電子ファイルキャビネットを管理するホストコンピュータであり、１１０は本システムにおけるワークステーションあるいはパーソナルコンピュータ、等の端末である。

【0005】図Ａのシステムの動作を以下説明する。端末１１０よりユーザＩＤが送出されると、ホストコンピュータ１００はパスワードファイル１０１からこのユーザＩＤに対応するパスワードＰＷを検索して出力する。

【0006】このパスワードＰＷはユーザＩＤに続いて端末から送られてくるパスワードＰＷと比較手段１０３により照合され、一致したときはシステムへのログインが許可される。

【0007】電子ファイルキャビネットへのアクセスはホストのログインとは別に管理されている。端末１１０からアクセスすべきキャビネット名を含むコマンドが送出されると、アクセスを制御する手段１０４は、ログインを許可したユーザＩＤと指定されたキャビネット名とによりアクセス管理テーブル１０５を検索する。

【0008】各ユーザＩＤにはキャビネット毎にリード，ライト，リライト等の権限が許可されているので、アクセス管理テーブル１０５を検索した結果により所定のアクセスを許可する。

3

【0009】

【発明が解決しようとする課題】上記の従来方式では以下の問題点が存在する。①回線盗聴によりパスワードが盗まれる危険性がある。

【0010】②パスワードファイルは厳重に保管しなければならない。③アクセス管理テーブルは厳重に保管しなければならない。④ファイルは暗号化されていない為に，盗み見の危険性がある。

【0011】これらの問題を解決する為に，回線の暗号化及びファイルの暗号化が必要となる。又，読み出しに対する保護としてはファイルの暗号化が考えられるが，書き換えに対する保護にかんしては，アクセス制御に頼る必要がある。

【0012】これらの技術については、互いに独立したものは実現している。例えばアクセス制御については、ファイルを暗号化／復号化するための鍵を作成し管理する技術が、本願出願人により特願昭01—184715号で提案している。

【0013】しかし、電子ファイルキャビネットのシステムにおいては、ログイン制御とアクセス制御を個別に管理しており、非常に複雑なものであった。本発明は、電子ファイルキャビネットシステムにおいて、ログイン制御とアクセス制御と一元的に管理することにより、管理を簡単にすると共に安全性の高い電子ファイルキャビネットシステムの提供を目的とする。

【0014】

【課題を解決するための手段】上記の課題を解決するためになされた本発明の電子ファイルキャビネットシステムは、ユーザ側の端末1と、該端末1から送出された要求に基づいてホストコンピュータ2が電子ファイルキャビネット29をアクセスするシステムにおいて、前記端末1側には、ユーザを識別するためのユーザ識別情報を入力して前記ホストコンピュータ2側に送出する手段11と、ユーザの秘密情報と前記電子ファイルキャビネットを特定化するファイル識別情報とを構成要素として含み作成された公開鍵を入力する手段12と、前記公開鍵とユーザにより入力される前記秘密情報とに基づいて第一の秘密鍵を生成する手段16と、入力された該認証情報を前記秘密鍵を用いて暗号化して前記ホストコンピュータ2に送出する手段17と、入力されたファイルアクセスコマンドを前記第一の秘密鍵を用いて暗号化して前記ホストコンピュータ2に送出する手段18とを有し、前記ホストコンピュータ2は、前記ユーザ識別情報毎にアクセス権限が与えられたファイルのファイル識別情報が格納されるユーザプロファイル21と、前記ユーザプロファイル21から読みだされる識別情報を基に第二の秘密鍵を作成する手段22，23，24と、前記第二の秘密鍵を用いて前記暗号化された認証情報を復号する手段25と、前記復号した認証情報の正当性をチェックして端末1のログインを許可／不許可を行う手段26と、

4

前記第二の秘密鍵を用いて前記暗号化されたコマンドを復号する手段27と、前記復号されたコマンドを基に前記ユーザプロファイル21を参照し、アクセス権限を確認して前記電子ファイルキャビネット29をアクセスするアクセス制御手段28を有することを特徴とするものである。

【0015】また、前記公開鍵は、所定の整数をベキ乗して得られるデータ値であり、該ベキ乗の項には前記秘密情報の逆数と前記識別情報の逆数とが積の項が含まれ、前記第一の鍵生成手段16は、入力された前記秘密情報を用いて前記公開鍵から前記秘密情報の逆数の項を消すことにより前記第一の秘密鍵を生成し、前記第二の鍵生成手段22，23，24は、センタ秘密情報23を用いて前記各識別情報の逆数を生成し、得られた各識別情報の逆数を項として用いて前記所定の整数のベキ乗演算を行うことにより第二の秘密鍵を生成するようにしても良い。

【0016】更に、前記ホストコンピュータ2は、前記ユーザプロファイル21中の各識別情報の項には該識別情報が更新されか否かを示す更新情報を設けると共に、更新された識別情報と更新される前の識別情報との対応関係を記憶する変更識別情報保持手段41を設け、受信したユーザ識別情報によりユーザプロファイル21から各識別情報を読みだす際には前記更新情報をチェックして、更新がなされている場合は前記変更識別情報保持手段41を読みだして得られる新しい識別情報を含む公開鍵生成情報を作成し、この公開鍵生成情報を前記第二の秘密鍵を用いて暗号化してログインを許可した端末に送出し、その後で前記ユーザプロファイル21のうち更新すべき識別情報の項を新しい識別情報に書換えるよう構成し、前記端末1は、前記暗号化された公開鍵生成情報を前記第一の秘密鍵を用いて復号して、公開鍵を更新するように構成しても良い。

【0017】

【作用】本発明の電子ファイルキャビネットシステムでは、まず各ユーザに対して、該ユーザの秘密情報（パスワード）と、ユーザ毎の識別情報（IDコード）とアクセス権限が与えられた電子ファイルキャビネットの識別情報（IDコード）とを用いて作成された公開鍵を供給する。

【0018】このユーザがホストコンピュータ側の電子ファイルキャビネットをアクセスする時は、まずユーザIDを入力する。これはホストコンピュータ2に送出される。

【0019】次に公開鍵とパスワードを入力する。これにより第一の鍵生成手段16は前記の公開鍵からパスワードに基づく項を取り除き、第一の秘密鍵を作成する。その後でユーザが認証番号（センタID）を入力すると、暗号化手段17はこの認識番号を第一の秘密鍵を用いて暗号化し、ホストコンピュータ2に送出する。

5

【００２０】一方ホストコンピュータ２はユーザＩＤを受信すると、このユーザＩＤに対応する各ＩＤコードを読みだす。次に読みだされた各ＩＤコードを用いて第二の秘密鍵を生成する。

【００２１】ここで第一の秘密鍵と第二の秘密鍵は予めセンタが取り決めた式により生成されるので、同じＩＤコードが用いられている場合は同じ値となる。つまり、ユーザはＩＤコードを入力して（ホストコンピュータ２により）第二の秘密鍵を生成し、一方パスワードを入力することにより公開鍵から第一の秘密鍵を生成する。

【0022】更にホストコンピュータ２が受け取った暗号化された認証番号は第二の秘密鍵を用いて復号される。この暗号化／復号の方法も取り決められているので、第一の秘密鍵と第二の秘密鍵が一致していれば、同じ認証番号が得られるわけである。

【００２３】この認証番号が正当なものであれば、ホストコンピュータ２は端末１のログインを許可する。さらにログインを許可されたユーザはキャビネットをアクセスするためのコマンドを入力すると、暗号化手段１８は第一の秘密鍵を用いて該コマンドを暗号化し、ホストコンピュータ２に送出する。

【００２４】これを受信したホストコンピュータ２側の復号手段２７は、第二の秘密鍵を用いてコマンドを復号する。（上記のように第一の秘密鍵と第二の秘密鍵とは一致する。）このコマンドに基づき、アクセス制御手段２８はユーザプロファイル２１を参照してアクセス権限が与えられているかのチェックを行い、キャビネット２９に対するアクセス許可を行う。

【００２５】また、キャビネットの鍵を変更する場合は、そのキャビネットの識別情報が変更されるので、それに基づきユーザ側の公開鍵も変更する必要がある。そこで、ユーザプロファイル２１の各識別情報にこの識別情報が更新されるものであることを示すフラグ等を設けてログイン時にこれを参照するようにする。そして更新すべき識別情報については変更識別情報保持手段３１よりこれを読みだし、この識別情報を含む新しい公開鍵生成情報を作成してこれを暗号化して現在ログインを許可した端末１に送出する。

【００２６】端末１では受け取った公開鍵生成情報を復号し、これにより公開鍵を更新する。

【００２７】

【実施例】以下図面を参照して本発明の実施例を説明する。図１は本発明の第一の実施例の説明図である。

【００２８】１は端末であり、２はセンタにあって電子＊

6

＊ファイルキャビネットを管理するホストコンピュータである。端末１は、ユーザ個人のＩＤを入力してホストコンピュータ２に送出するユーザＩＤ入力手段１１、ユーザの所属部ＩＤ，所属課ＩＤ，従事しているプロジェクトＩＤ等のＩＤの逆数とパスワードの逆数とにより生成される公開鍵を入力する手段１２、パスワードを入力する手段１３、センタＩＤや日時や乱数を入力する手段１４、ホストコンピュータ２側の電子キャビネットのアクセスを指示するコマンド入力手段１５、公開鍵入力手段から送出される公開鍵と入力されたパスワードとにより第一の秘密鍵を生成する秘密鍵生成手段１６、センタＩＤ，日時，乱数を第一の秘密鍵を用いて暗号化する手段１７、コマンドを第一の秘密鍵を用いて暗号化する手段１８とにより構成されている。

【００２９】ホストコンピュータ２は、ユーザ個人のＩＤと対応する所属部ＩＤ，所属課ＩＤ，プロジェクトＩＤ等とが格納されるテーブルであるユーザプロファイル２１、ユーザプロファイル２１から読みだされたＩＤコードとセンタが持つ秘密情報２３よりＩＤコードの逆数を生成するＩＤ逆数生成手段２２、生成された各ＩＤの逆数を用いて第二の秘密鍵を生成する鍵生成手段２４、第二の秘密鍵を用いて端末から送出される暗号化されたセンタＩＤ等の複号を行う複号手段２５、複合化されたセンタＩＤの正当性をチェックする手段２６、第二の秘密鍵を用いて暗号化されたコマンドの複号を行う複号手段２７、複号されたコマンドに基づきユーザプロファイル２１に基づいてアクセス権限のチェックを行い、アクセス許可したものについて電子ファイルキャビネット２９のアクセスを制御する手段２９とにより構成されている。

【００３０】なお公開鍵入力手段１２は、例えばセンタから各ユーザに公開鍵を記録した磁気カードまたはＩＣカード等を配付し、この媒体を用いて入力するよう構成する。またユーザＩＤ入力手段１１、パスワード入力手段１３、センタＩＤ等の入力手段１４、コマンド入力手段１５は実際は同じキーボード等の入力装置であり、暗号化手段１７，１８は同じものを使用している。同様にホストコンピュータ２の複号手段２５，２７も同じものが使用される。

【００３１】センタから予め供給される公開鍵は、例えば下記のものが用いられる。

【００３２】

【数１】

$$PW^{-1} \times \text{ユーザＩＤ}^{-1} \times \text{所属部ＩＤ}^{-1} \times \text{所属課ＩＤ}^{-1} \times \text{プロジェクトＩＤ}^{-1} \quad M$$

【００３３】これはパスワードＰＷの逆数と各ＩＤデータの逆数との積を用いてセンタが決定する定数Ｍのベキ乗演算するものである。また秘密鍵は、下記のものが用いられる。

【００３４】

【数２】

7　　8

ユーザID^{-1}×所属部ID^{-1}×所属課ID^{-1}×プロジェクトID^{-1}

M

【0035】これは端末1側では入力されたパスワードPWを用いて、公開鍵のベキ乗項からパスワードの逆数を取り除くことにより生成される。一方ホストコンピュータ2側では、ユーザプロファイル21に格納されている各IDの逆数が生成されて、この各IDの逆数の積により前記Mのベキ乗演算を行い生成される。

【0036】この逆数の生成方法であるが、例えばセンタ秘密情報で素数p，qを用意し、逆数生成手段は、

【0037】

【数3】

$$D^{-1} = 1 \mod \{LCM[(p-1)(q-1)]\}$$

【0038】等の関係を使って求める。なお、modは剰余計算を意味し、LCMは最小公倍数を求める演算を意味する。また、各暗号化手段17，18および複号手段25，27は、公知の暗号化方法であるDES，FEAL等を用いるものである。

【0039】次に図1にしめした一実施例の動作を説明する。①端末1側にいるユーザは、ホストコンピュータ2にユーザID入力手段11を用いてユーザIDをおくるとともに，公開鍵入力手段12からの公開鍵とパスワード入力手段13からのパスワードとを用いて鍵生成手段16が第一の秘密鍵を生成する。

【0040】②ホストコンピュータ2は、送られてきたユーザIDよりユーザプロファイル21を参照する。このユーザのプロファイルに書かれている所属部ID等の各IDは逆数生成手段22によりセンタ秘密情報を用いて逆数が生成される。

【0041】この各IDの逆数を用いて鍵生成手段24は第二の秘密鍵を生成する。③ユーザがセンタID，日時，所定の乱数を入力手段14を用い入力すると、端末1の暗号化手段17は（センタコード＋日時＋乱数）を第一の秘密鍵16を用いて暗号化しホストコンピュータ2に送信する。

【0042】④ホストコンピュータ2の複号手段25は暗号化された（センタコード＋日時＋乱数）を鍵生成手段24により生成された第二の秘密鍵を用いて複号し、このコードの正当性をチェック手段26がチェックして正当なセンタコードが得られたらログインを許可する。

【0043】⑤ログインが許可された旨は図示しない手段により端末1に通知されるので、ユーザはこれを受けてコマンドを入力手段15を用いて入力する。このコマンドにより、実行すべきアクセスの種類（リード，ライト等）と、アクセスするキャビネット名が指定される。

【0044】コマンドは暗号化手段18が第一の秘密鍵を用いて暗号化されてホストコンピュータ2に送出される。⑥ホストコンピュータ2ではこの暗号化されたコマンドを受信すると第二の秘密鍵を用いて復号手段27を用い復号しコマンドを得る。アクセス制御手段28はユーザプロファイル21を参照し、コマンドで指定されたアクセスに対する権限が与えられているかのチェックを行う。

【0045】アクセス制御手段でアクセスの権限が確認されたならば，キャビネット29へのアクセスが可能となる。次に本発明の第二の実施例を図2を用いて説明する。

【0046】本実施例は電子ファイルキャビネットシステムにおいてIDを変更する方法に関するものである。このシステムは基本的には図1に示した第一の実施例と同一のものを用いているが、本実施例と直接の関係がない部分については図2では省略している。

【0047】キャビネットの鍵を変更する場合には，キャビネットのIDを変更する必要がある。しかしキャビネットのIDをシステム側で変更した場合も、ユーザ側の公開鍵はこのIDコードの情報を基に作成されているので、この公開鍵を変更する必要が生じる。

【0048】ここでプロジェクトのキャビネットの鍵が変更になった場合を例として説明する。①第一の実施例と同様にホストコンピュータ2へのログインを行なう。

【0049】②ホストコンピュータ2側で、ログインしたIDに対してのユーザプロファイル情報に対して変更の情報を持っていたならば、新しいプロジェクトID及び他のIDより新しい鍵生成情報44を生成する。これは例えばユーザプロファイル21に更新フラグを設け、この値により変更識別情報保持手段31を検索してプロジェクトID2がID3になっていることを検索して出力する。そして鍵生成手段32は新しいIDと他のIDとシステム側で保持しているユーザのパスワードとにより新しい公開鍵生成情報を作成する。

【0050】③公開鍵作成手段は復号手段33により第二の秘密鍵を用いて暗号化され、端末1に送信する。④端末1では、これを復号手段41により復号し公開鍵生成情報を得る。そして公開鍵生成手段42は磁気カード等の媒体に記録されている現在の公開鍵を新しい公開鍵に書き換える。

【0051】⑤ホストコンピュータでは、アクセスしたユーザプロファイルのうち、プロジェクトIDに関する部分を新しいIDに書き換える。

【0052】

【発明の効果】以上説明したように、本発明の電子ファイルキャビネットシステムによれば、複数のユーザがアクセス可能なキャビネットへの鍵の管理が可能になり、又、ログイン制御、アクセス制御等も同じ仕組みの上で成り立つことが可能となるので、安全性が高く、かつ管理が容易になる。

9

【図面の簡単な説明】

【図1】本発明の電子ファイルキャビネットシステムの第一の実施例である。

【図2】本発明の電子ファイルキャビネットシステムの第二の実施例である。

【図3】従来の電子ファイルキャビネットシステムの一例を示す図である。

【符号の説明】

1　ユーザ側端末

2　ホストコンピュータ

10

11　ユーザ識別情報入力手段

16　第一の鍵生成手段

17，18　暗号化手段

21　ユーザプロファイル

22，23，24　第二の鍵生成手段

25，27　復号手段

28　アクセス制御手段

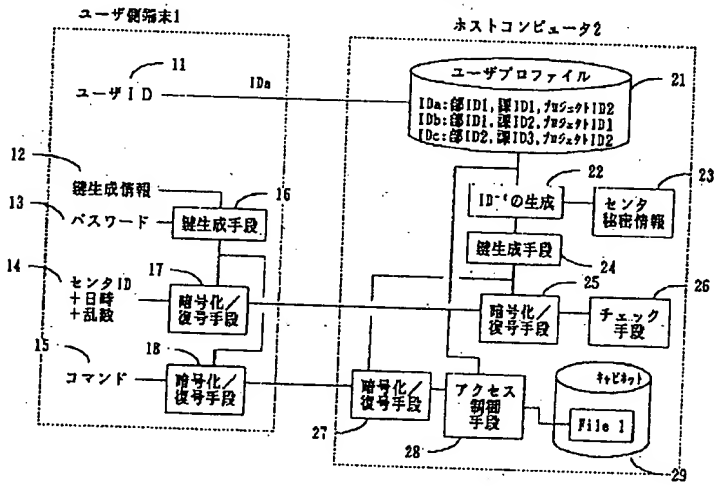
29　電子ファイルキャビネット

31　変更識別情報保持手段

10

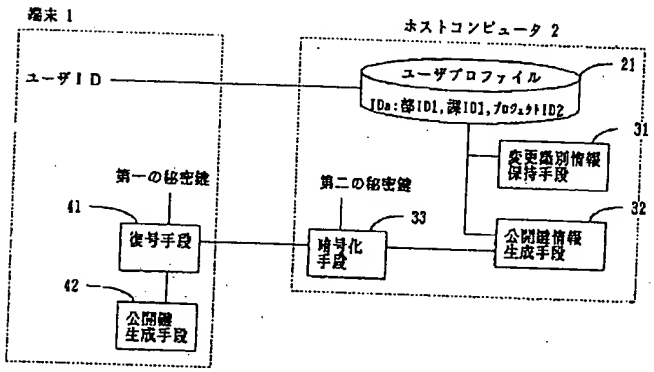
【図1】

本発明の第一の実施例の構成を示す図



【図2】

本発明の第二の実施例を示す図



【図3】

従来の電子ファイルキャビネットシステムの一例を示す図